UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/542,630	04/24/2006	Christian Benardeau	0512-1290	1731

466 7590 12/04/2009

YOUNG & THOMPSON
209 Madison Street
Suite 500
Alexandria, VA 22314

EXAMINER	
ARMOUCHE, HADI S	

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
12/04/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DocketingDept@young-thompson.com

Office Action Summary	Application No.	Applicant(s)	
	10/542,630	BENARDEAU, CHRISTIAN	
	Examiner	Art Unit	
	HADI ARMOUCHE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 September 2009*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3 and 5-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3 and 5-20* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This communication is in response to applicant's remarks filed on 09/02/2009. No claims have been amended. Claims 1-3 and 5-20 remain pending.

Response to Arguments

2. Applicant's arguments filed 09/02/2009 have been fully considered but they are not persuasive.

3. It has been argued (page 14 of the remarks) that Menezes does not teach an authentication code (MAC/identifier) for a computer software program. Instead, Menezes teaches an authentication code for a message.

4. Applicant's interpretation of the reference is noted. However, the examiner respectfully disagrees. The rejection was structured so that the two references (Maillard and Menezes) would be taken in combination. Maillard teaches the transmission of a computer program while Menezes teaches sending a message with a MAC for verification. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Maillard to prevent the usage of information found to be incomplete or inaccurate, as found in Menezes, in order to prevent the corruption of the received data.

5. It has been argued (pages 14 and 15 of the remarks) that Menezes does not describe the use of a single identifier for a group of several programs to be transmitted, nor that this identifier is calculated from information relating to each of the software programs of the group.

6. Applicant's interpretation of the reference is noted. However, the examiner respectfully disagrees. Menezes teaches that the MAC *h*(x) is computed over the entire message (with all its data and information) to be transmitted and transmit the message along with its MAC. The recipient recalculates the MAC for the message and compares it with the MAC received to make sure that the message has not been altered. The message (as discussed earlier in point 4 above) can be a computer program or programs since a message is a data and packets. Moreover, the claim indicates *"transmitting the* *<u>at least one</u>* *computer software program to the at least one encryption/decryption module of the decoder".* Therefore, the transmitter can send only <u>one</u> software program and not a group of programs. In other words, the "group" of software programs is understood to be consisting of one software program.

Claim Rejections - 35 USC § 103

7. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

8. Claims 1-3, 5, 9-13, 15-17, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard, et al. (US 2002/0129249), hereafter referred to as Maillard, in view of Menezes, et al. *Handbook of Applied Cryptography*. Boca Raton, FL. CRC Press LLC, 1997, hereafter referred to as Menezes.

<u>Regarding claims 1 and 12:</u>

Maillard [0102] teaches a transmitter that encrypts broadcast information.

Maillard [0097], [0099] teaches the generation and transmission of a control word which is necessary for the decryption of the encrypted information.

Maillard [0101]-[0104] shows the scrambled information being sent from the transmitter to the end user's receiver/decoder.

Maillard [0231] shows that the system can include a checksum for the purposes of data integrity.

However, Maillard fails to explicitly disclose a system that transmits an identifier along with the scrambled data to verify the integrity of the data.

Menezes page 364, section 9.6.3 teaches data integrity using a MAC. The sender computes the MAC and transmits it to the receiver. The receiver then uses the MAC to make sure that the data has not been altered in transit.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Maillard to prevent the usage of information found to be incomplete or inaccurate, as found in Menezes, in order to prevent the corruption of the received data.

Regarding claim 2:

Maillard [0097], [0099] shows a system that encrypts a control word necessary to decrypt the data at the corresponding receiver/decoder.

Regarding claims 3, 16, and 19:

Maillard [0231] shows that the system can include a checksum for the purposes of data integrity.

Menezes page 364, section 9.6.3 teaches data integrity using a MAC. The sender computes the MAC and transmits it to the receiver. The receiver then uses the MAC to make sure that the data has not been altered in transit.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Maillard to prevent the usage of information found to be incomplete or inaccurate, as found in Menezes," in order to prevent the corruption of the received data.

Regarding claim 10:

Maillard [0091], [0092] and Fig. 2 shows a "mother" smartcard connected to the ciphering units. The mother smartcard controls the operation of the ciphering unit.

Regarding claims 11, 13, and 17:

Maillard [0091], [0092] and Fig. 2 shows a "daughter" smartcard connected to the receiver/decoder units. The daughter smartcard controls the operation of the receiver/decoder unit.

Regarding claim 15:

Maillard [0102] teaches a transmitter that encrypts broadcast information.

Maillard [0097], [0099] teaches the generation and transmission of a control word which is necessary for the decryption of the encrypted information.

Maillard [0101]-[0104] shows the scrambled information being sent from the transmitter to the end user's receiver/decoder.

Maillard [0231] shows that the system can include a checksum for the purposes of data integrity.

9. Claims 5 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard in view of Menezes and further in view of Booth, et al. (WO 01/61437 A2), hereafter referred to as Booth.

Regarding claim 5:

Maillard and Menezes teach the "method according to claim 3", (see above rejection), but fail to explicitly state that steps d), g), h), i), and j) are carried out by the same encryption/decryption module.

However, **Booth page 6, lines 22-26** shows a single secure processor for carrying out the various security authentications.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Maillard to allow a single processor to carry out the various validation functions, as taught by Booth, in order to minimize the use of system resources and promote the use of specialized components within the computing device.

Regarding claim 9:

Maillard and Menezes teach the “method according to claim 2”, (see above rejection), but fail to explicitly disclose that the system carries out the computer software program each time the integrity thereof is validated.

However, **Booth page 17, lines 18-30** shows that the master processor can access or execute authenticated sections of code as needed.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Maillard to only execute sections of code after the integrity of the code is verified, as taught by Booth, in order to prevent inadvertent or malicious misuse of the computer system.

10. Claims 14 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard in view of Menezes and further in view of Gammie (US 5,029,207), hereafter referred to as Gammie.

Regarding claims 14 and 18:

Maillard and Menezes teach a “decoder according to claim 16” (see above rejection), but fail to explicitly disclose the decoder containing two autonomous encryption/decryption modules, independent of each other, where at least one is fixed to the body of the decoder.

However, **Gammie column 10, lines 4-10 and Fig. 7** shows a decryption module with both an internal and external security device. The external security device is removable.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Maillard to use both internal and external security modules for increased piracy protection as described in Gammie. An internal security module, provides protection against physical alteration of the decoder/receiver and an external module allows for easy security upgrades and termination of compromised modules.

11. Claims 6-8 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard in view of Menezes and further in view of Nagae (US 5,598,530), hereafter referred to as Nagae.

Regarding claims 6 and 20:

Maillard and Menezes teach the “method according to claim 4,” (see above rejection) but fail to explicitly disclose that the first module carries out only steps d), h), i), and j), and that the second module carries out at least step g).

However, **Nagae column 3, lines 16-37 and Fig. 1** shows a system where a calculating unit calculates a checksum, then a separate unit compares the checksum with an already stored checksum value. The control unit executes the program if the comparison is positive and inhibits and deletes the data if the comparison is negative.

It would have been obvious to one of ordinary skill in the art at the time of invention to modify Menezes to include a separate unit used solely for computing a checksum, as described in Nagae, as it reduces the number of calculations performed by each unit and allows each unit to synchronously perform additional tasks while waiting for output from the other.

Regarding claim 7:

Maillard [0041] and [0095]-[0100] shows control signals being sent to the receiver/decoder that prevent the decoding of the information if the user doesn't have the proper rights. This process is done in addition to the error checking process.

Regarding claim 8:

Maillard [0095]-[0100] shows that access criteria and control words are sent in one common ECM.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to HADI ARMOUCHE whose telephone number is (571)270-3618. The examiner can normally be reached on M-Th 7:30-5:00 and Fridays half day.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/H. A./
HADI ARMOUCHE
Examiner, Art Unit 2432

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432